

IN THE UNITED STATES DISTRICT COURT
FOR HELENA, MONTANA

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
wkbrdr1994@gmail.com THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE INC.

Case No. MS-12-3-H-RKS

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

Affiant, Aaron M. Reller, being duly sworn, depose and state as follows, to wit:

1. Affiant makes this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Google Inc., an email provider located at 1600 Amphitheatre Parkway, Mountain View, CA., 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.
2. Affiant is a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, presently assigned to the Resident Agent in Charge, Helena, Montana and has been employed since May 1996.
3. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations 18 U.S.C. § 2252A(a)(5), which, among other things, makes it a federal crime for any person to access with intent to view child pornography, and 18 U.S.C. § 2251(a)

and (e), which makes it a crime to attempt to produce child pornography.

4. The statements contained in this Affidavit are based on Affiant's experience and background as a Special Agent and on information provided by other law enforcement agents.
 - a. In addition to Affiant's experience as a Homeland Security Special Agent, your Affiant has received a Bachelors Degree from Montana State University in Bozeman, Montana. Affiant is responsible for conducting federal and international investigations relating to crimes involving the sexual exploitation of children, including investigations related to online child exploitation. Affiant has received basic, advanced, and on-the-job training in the investigation of cases involving the sexual exploitation of children.
5. Because this Affidavit is submitted for the limited purpose of securing a search warrant, Affiant has not included each and every fact known to him concerning this investigation. Affiant has set forth only those facts which Affiant believes are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. § 2252A(a)(5) and 18 U.S.C. § 2251(a) and (e) have been committed by the person or person(s) using wkbrdr1994@gmail.com.
6. Based upon Affiant's knowledge, training, and experience, as well as information related to the Affiant by agents and others involved in the forensic examination of digital devices, the Affiant knows that:
 - a. Digital evidence, by its very nature, is fragile and can be altered, damaged, or destroyed by improper handling or examination.
 - b. A person who receives, possesses, and distributes child pornography, which is contraband per se, is likely to destroy evidence of the illegality by attempting to delete files from the computer media, which may or may not be recoverable, or dispose of the physical hard drive in its entirety.

- c. The spoliation of original evidence may be detrimental to the investigation of the case because, in the course of an examination of computer hard drives, the imaging or examining agent may need to re-image original media in the case of image corruption.
- d. Permitting the target of an investigation to retain control over the original media (hard drive) after imaging would require the seizing and/or imaging agent to “wipe” or forensically delete any child pornography from the hard drive, and on-site technological capabilities cannot ensure a complete “wipe” of child pornography and trace evidence of child pornography from a computer.
- e. Permitting the target of an investigation to retain control over original evidence that may contain child pornography or traces of child pornography after being “scrubbed” is inconsistent with 18 U.S.C. §3509(m), which requires that the Government maintain control over contraband involving child pornography.

PERTINENT CRIMINAL STATUTES

- 7. This investigation concerns alleged violations of 18 U.S.C. § 2252A, relating to material involving the sexual exploitation of minors.
- 8. 18 U.S.C. § 2252A(a)(5) knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;
- 9. 18 U.S.C. § 2251(a) and (e) prohibits a person from attempting to

knowingly employ or use any minor to engage in sexually explicit conduct, including the lascivious exhibition of the genitals or pubic area, for the purpose of producing any visual depiction of such conduct, knowing and having reason to know that such visual depiction would be transported using any means and facility of interstate and foreign commerce, or using materials that have been mailed, shipped, and transported in and affecting interstate and foreign commerce by any means, including by computer.

DEFINITIONS

10. The following non-exhaustive list of definitions applies to this Affidavit and Attachments A and B to this Affidavit:
 - a. “Child Pornography” includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).
 - b. “Visual depictions” include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image, whether or not stored in a permanent format. See 18 U.S.C. § 2256(5).
 - c. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).
 - d. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic

abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

- e. “Computer” as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1), as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.”
- f. “Computer hardware” as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory or optical storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware and software (including, but not limited to, physical keys and locks and dongles or other electronic access devices).
- g. “Computer software” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- h. “Computer-related documentation” as used herein, consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, computer software, or other related items.

- i. “Computer passwords and data security devices” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alphanumeric characters) usually operates a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, dongles, and circuit boards. Data security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.
- j. “Internet Service Providers” or “ISPs” as used herein, is defined as a business that allows a user to dial into or link through its computers allowing the user to connect to the Internet for a fee. Typically, the customer pays a monthly fee and the ISP supplies software that enables the customer to connect to the Internet by a modem or similar device attached to or installed in a computer.
- k. “ISP Records” are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e-mail communications, information concerning content uploaded and/or stored on or via the ISP’s servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers’ use. This service by ISPs allows for both temporary and long-term storage of electronic communications

and many other types of electronic data and files.

- l. "Internet Protocol address" or "IP address", as used herein, is defined as a numeric address of a machine in the format used on the Internet. The IP address is a unique number consisting of four blocks of numbers as in 123.456.789.001, for example.
- m. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, including unallocated or deleted data, whether in handmade form, photographic form, mechanical form or electrical, electronic, optical, or magnetic form (including, but not limited to, tape recordings, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, Personal Digital Assistants (PDAs), flash memory devices, optical disks, smart cards, as well as digital data files and printouts or readouts from any magnetic, optical, electrical or electronic digital device).
- n. "Digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: computers; central processing units; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile or cellular phones; smart phones; digital cameras; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related computer communications devices such as modems, routers, network access devices, and connections; storage media such as internal and external hard drives, floppy disks, optical discs, flash memory devices, magnetic tapes; and security devices.
- o. "Image" or "forensic copy" refers to an accurate reproduction of information contained on an original physical item, yet is independent of the electronic storage device.
- p. "Hash value" refers to a mathematical algorithm generated

against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data.

**CHILD PORNOGRAPHY, COMPUTERS AND
THE ONLINE EXPLOITATION OF CHILDREN**

11. Based upon Affiant's knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom Affiant have had discussions, the Affiant is aware of the following:
 - a. Individuals involved in the sexual exploitation of children often possess and maintain for many years records, documents and materials depicting child pornography. They may receive sexual gratification from viewing children engaged in sexual activity or in sexually suggestive poses.
 - b. Computers and computer technology have revolutionized the way in which child pornography is produced, distributed, stored and communicated as a commodity and a further tool of online child exploitation. Computers and related storage devices such as external hard drives and flash drives serve a number of functions in connection with child pornography, to include advertisement, distribution, and storage. These devices can be very small and portable. They can easily be hidden in a person's residence, vehicle, or on their body.
 - c. Child pornography is not readily available in retail establishments in the United States, because it is illegal. Accordingly, individuals who wish to obtain child pornography often do so by ordering it from abroad or by discreet contact with other individuals who share their interests and have it available. The use of computers to traffic in, trade or collect child pornography has become one of the preferred methods of obtaining these materials. An individual familiar with a

computer can use it in some private location to interact with another individual or a business offering such materials. The use of the computer offers individuals interested in obtaining child pornography a sense of anonymity, privacy and secrecy not available elsewhere, as well as the added benefit of speedy transmissions and communications. These individuals often try to hide their interest in child pornography, as well as their collection, by carrying it with them on a portable electronic device or laptop.

- d. One of the most efficacious ways to expand a collection of child pornography is to offer another collector, via posting to a board or a trade over the Internet, images that the trading partner does not already possess. Accordingly, it may be necessary to keep a great number of images in storage so as to have adequate material to allow participation in this informal barter system and thus collectors involved in sending or receiving child pornography may retain it for long periods of time. This tendency is enhanced by the increased sense of security that a computer and peripherals provides. In addition to the emotional value the images have to the collector, the images of child pornography are intrinsically valuable to trade and/or selling and therefore are rarely destroyed or deleted by a collector. Individuals may also visit free or pay websites, and repeatedly view child pornography images and movies that need not be saved or downloaded to their computer. Computer forensics technicians may be able to extract the images and movies that were viewed at these websites or traded via the Internet. Individuals who procure child pornography may try to keep such material in their residence or other secure locations to ensure convenient and ready access.
- e. Today, laptop computers can have very large storage capacity and fast processing systems. Laptop computers are mobile. If users are utilizing a laptop computer, the users will frequently take the laptop computer with them or in their vehicle when they leave their residence.

EVIDENCE ASSESSMENT PROCESS AND OFF-SITE ANALYSIS

12. Based on Affiant's knowledge, training and experience in these types of investigations, and the experience and training of other agents with whom Affiant have had discussions, Affiant knows the following:
 - a. Searches and seizures of evidence from computers require investigators to seize most or all computer items (hardware, software, passwords and instructions) to be processed later by a qualified computer expert in a laboratory or other controlled environment. Computer storage media to include but not limited to floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process renders it impractical to attempt this kind of data search on site.
 - b. Searching computer systems for criminal evidence requires experience in the computer field and properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both for external sources and from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.
 - c. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the computer. In cases like this one where the evidence consists

partly of graphics files, the input and output devices to include but not limited to scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media are also essential to show the nature and quality of the graphic images which the system could produce. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware devices) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as documentation, items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software.

- d. Persons trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a persons interest in child pornography or child exploitation.
- e. Files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files.
- f. Computer software or hardware exists that allow persons to share Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.
- g. Computers used to access the Internet usually contain files, logs

or file remnants which would tend to show ownership and use of the computer as well as ownership and use of internet service accounts used for the internet access.

- h. Search warrants of residences involved in computer related criminal activity usually produce items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts access to obtain child pornography to include credit card bills, telephone bills, correspondence and other identification documents.
 - i. Search warrants of residences usually reveal items that would tend to show dominion and control of the property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.
- 13. Based upon Affiant's knowledge, training, and experience, as well as information related to Affiant by agents and others involved in the forensic examination of digital devices, Affiant knows that establishing a prospective, pre-execution search protocol in this investigations is not practical because computer searches involve a dynamic process of electronic data review and information sharing between the examining agent and agents involved in the investigation. Only after the examining agent determines the appropriate search protocol based upon his/her assessment of the specific evidence does the examining agent develop the search protocol and begin the forensic search of the digital evidence. During the course of that review, the protocol may change. Therefore, this information could not be included in a prospective, pre-execution search warrant protocol.

INTERNET ACCESS AND TECHNOLOGY

- 14. Based upon Affiant's knowledge, training and experience and the experience of other law enforcement personnel, Affiant is aware that many computer users obtain access to the Internet via a wireless router. This gives them the ability to access the internet beyond the confines

of their home. In addition, computer technology is ever changing. Sophisticated users, such as the suspected user identified below, frequently update their computers and media. Based on my experience conducting searches of this nature, older computers and storage devices are sometimes maintained by the user in garages prior to destruction or recycling. As such, mobile media to include computers, cell phones, smart phones and thumb-drives, which are used as internet access and storage devices, have been known to be located in areas of the property other than the house including garages, cars and on people. Because some of the devices are mobile and some are very small, they can easily be carried in a car or on a person's body.

DETAILS OF THE INVESTIGATION

15. Some of Affiant's knowledge of the following details of investigation come from other law enforcement agents and personnel, and include but are not limited to background information, investigative techniques, and other evidence retrieved during the course of the investigation.
16. On or about November 29, 2011, The Department of Homeland Security (DHS) Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Cyber Crimes Center, Child Exploitation Investigations Unit (C3 CEIU) received information from the Danish National Police Service regarding a bulletin board accessible through Tor (The Onion Router) designed to facilitate the receipt and distribution of child pornography. The bulletin board was purported to be operated by "Falko" a child pornography producer. On the board, Falko offers access to a "VIP" area, where he posts newly produced child pornography. Falko also offers newly produced child pornography videos for sale.
17. The bulletin board is titled "Falkovideo" and operates only on Tor. This board is divided into two sections, the free area and the VIP-private section. As described by "Falko" in the free area you can talk with members as well as upload and download content. In the VIP-private section "Falko" states that you will gain access to his video

and photo content that is updated weekly and is not available in the free area. As a VIP member you also gain access to content in the VIP-private area that other members have uploaded.

18. C3 CEIU agents have joined the board and have downloaded images and movies depicting the sexual exploitation of minors. Some of this content appears to be “new” material and is alleged to be created by various members of the board including, but not limited to, Falko. This board has thousands of members, a vast majority of whom are not contributors but merely accessing and obtaining content from contributing members. Approximately one hundred fifty users are responsible for the nearly two thousand posts on the board. Of these, approximately eighty percent are attributable to a couple dozen users. This is a live active board and exact numbers change daily.
19. The address for the board is “fq niz5flbpwx3qmb.onion”(this is a Tor Hidden Service as described below). When first accessing the board, even before registering for the site, users will see a banner that depicts a prepubescent female child whose genital area is spread in a lewd and lascivious manner as well as the name of the board “Falkovideo”. This banner is visible on every page of the board. Without registering for the site, users are still able to access some topics on the board that both display images and provide links for videos, typically in .rar format. The password for the files is typically provided with the link if they are password protected files. The files are usually password protected unless they are embedded images on the post. When registering for the board users must create a username, password and provide an e-mail address. There is no validation for this registration process and the e-mail account does not have to be a valid e-mail.
20. To access the board, one must first install Tor as the board is only accessible through Tor as it is a Hidden Service. Tor (short for The Onion Router) was originally designed, implemented, and deployed as a third generation onion routing project of the U.S. Naval Research Laboratory, as a circuit-based low-latency anonymous communication service. It was originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications.

21. Information documenting what Tor is and how it works is provided on the Tor website at torproject.org. Additional documentation can be found at freehaven.net. The name "Tor" can refer to several different components. The Tor software protects users by bouncing their communications around a distributed network of relays run by volunteers all around the world: it prevents somebody watching their Internet connection from learning what sites they visit, it prevents the sites they visit from learning their physical location, and it lets them access sites which could otherwise be blocked.
22. Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features, such as Torbutton and Torbrowser bundle. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.
23. Tor makes it possible for users to hide their locations while offering various kinds of services, such as web publishing or an instant messaging server. Using Tor "rendezvous points," other Tor users can connect to these hidden services, each without knowing the other's network identity. A hidden service needs to advertise its existence in the Tor network before clients will be able to contact it. Therefore, the service randomly picks some relays, builds circuits to them, and asks them to act as introduction points by telling them its public key. By using a full Tor circuit, it's hard for anyone to associate an introduction point with the hidden server's IP address. While the introduction points and others are told the hidden service's identity (public key), they are not able to identify the hidden server's location (IP address). A hidden service can be recognized by the (hash value).onion address as is the case with the Falko board with the address "fqniz5flbpwx3qmb.onion".
24. With traditional internet investigations identifying the suspect behind alleged criminal activity is accomplished by tracking the action to the

internet service utilized by the suspect, more specifically by identifying the IP address used. The IP address tied to the activity can be identified in many ways ranging from logs from the source such as the server the material is accessed from, through session logs relating to the application used to access or transmit the data such as e-mail, file sharing, webcams or other services that require the user to sign up for an account.

25. While Tor masks the IP address of the user, there are other operations that occur with internet connectivity which can "leak" information that would identify the user behind Tor. Java, Javascript, Macromedia Flash and Shockwave, QuickTime, RealAudio, ActiveX controls, and VBScript are all known to be able to access local information about your operating system and local network. These technologies will work over proxies and can tunnel the information back to their source.
26. Youtube and similar sites require third party browser plugins such as Flash. Plugins operate independently from Firefox and can perform activity on your computer that ruins your anonymity. This includes but is not limited to: completely disregarding proxy settings, querying your local IP address, and storing their own cookies.
27. On April 10, 2012, a member of the board utilizing the username "wkbrdr16" was discovered to have posted content on the board in the form of image files.
28. On April 5, 2012, a member of the Falkovideo board using the username "wkbrdr16" started a thread within the Video forum of the board titled "NEW!! Family changing room spycam!!! (for VIP)." The post stated:
 - a. "I hope you guys enjoy. This one is just a little teaser. I know the guy personally who took these so I know they've never been seen before. I have much better ones to come!"
29. The post contained a link to a file hosting site called uploadorb.com

and a password to open the encrypted file once downloaded. The post also contained a thumbnail image of the file.

- a. A review of the file titled
“9cc1efe753654fa0220a77e5c3c14478.jpg” depicts what appears to be a still frame from a hidden video camera in a family changing room / bathroom. The walls of the room are green in color. A prepubescent female child is visible from the chest down and her genital area is exposed. Another prepubescent female child is partially visible wearing a diaper and nothing else in the room as well as the clothed legs of an adult. The video that was attached to the post was downloaded by C3/CEIU and was listed as “0306”. The video depicted a video of two prepubescent females walking around a green dressing room. One of the minors has a diaper on, but the other minor female’s genitalia is exposed. The minor female who is naked is shown to be going to the bathroom, and then both minor females are shown being dressed to go swimming. One adult/older child male is shown getting changed, but does not show any genitalia, while one adult female is also changing and her exposed breasts are shown.
30. Also on April 5, 2012, wkbrdr16 posted two additional image files and wrote “Here’s a little preview of things to come:”
 - a. The first image file is titled
“90d5f5a2b1e6803228372a6f94ce2e1f.jpg” and depicts a prepubescent female child in a green dressing room looking at her exposed genitalia.
 - b. The second image file is titled
“8e4da5ab9b26eccc3197669d4bafb1ff” and depicts a prepubescent with exposed genitalia getting dressed in a green dressing room.
31. On April 10, 2012, C3 CEIU verified that wkbrdr16 registered their forum email address as wkbrdr1994@gmail.com and sent an

administrative summons to Google for the registration and log data of the email address wkbrdr1994@gmail.com. C3 CEIU received the return from Google on May 11, 2012.

32. Google was unable to provide any Internet Protocol (IP) logs for the email account. However, the Google Subscriber Information included the user generated account name "Luke Thomas", and indicated that the account was generated on June 11, 2010 from an IP address belonging to Internet Service Provider (ISP) Optimum Online/Cablevision Systems. Optimum Online/Cablevision Systems would not have subscriber information associated with the IP address from 2010 because they retain user IP log data for one year.
33. On May 14, 2012, C3 CEIU Intelligence Research Specialist (IRS) Lauren Blue performed open source research to find information associated with the email address wkbrdr1994@gmail.com and username wkbrdr16. IRS Blue found multiple accounts and postings associated with the email address and username, which included:
 - a. An account in the name of wkbrdr16 on Stickam.com with a profile image of a young man with dirty blonde hair in a white collared shirt and a silver necklace.. The image name "Luke Thomas.jpg" is displayed below the image of the young man on the Stickam wkbrdr16 profile. The account was created on June 13, 2010, and last logged into on June 22, 2011. C3/CEIU served DHS summons 354/12 on the Stickam account on May 14, 2012. C3/CEIU received the ISP return on May 18, 2012. The return included registration and log data for the wkbrdr16 account. The account was registered to the email address wkbrdr1994@gmail.com on June 13, 2010. The most recent log data was from the IP address 174.44.165.69 on June 23, 2011 at 00:42 GMT. This IP address belongs to Optimum Online/Cablevision.
 - b. An account in the name of wkbrdr16 on the website blogtv.com. The user created the account on June 11, 2010, and last logged in on June 22, 2011. The user included the same profile image

as on the wkbrdr16 Stickam profile.

- c. An account in the name of WKBRDR16 on the Russian file sharing site imsrc.ru. The account was registered on April 27, 2011 with the name "Uncle Chester" and the email address wkbrdr1994@gmail.com. The account contains two photo albums with the names "Summer Time!", and "Around the house". The albums contain a total of eleven images, eight and three respectively. The images were posted on April 27, 2011. The eight images in the album "Summer Time!" include seven images of twin girls in bikini bathing suits at what appears to be at a sandy playground in a city environment with palm trees. The girls appear to be twelve to thirteen years old. The eighth image is of another girl in a bikini, who appears to be eleven to thirteen years old. The three images in the album "Around the house" are of what appears to be two clothed girls under the age of fourteen, showing their legs spread apart with views of what appears to be their under garments. The third image looks like the two clothed girls in a bed together.
- d. A user profile in the name of wkbrdr16 on the Philippine site kst.ph. The profile indicates that a comment was made regarding "Nudist Movie: Christmas Youth Party – DVDRip". It appears that users gain a "reputation" and points based upon posts that they make to the site.
- e. A Twitter account in the name of Luke Thomas (lukethomas1994). C3/CEIU found publicly available information regarding the account activity. The user joined various chats from July 2010 through August 2010. The earliest activity listed was on July 13, 2010 when Luke Thomas @lukethomas1994 joined a video chat at [#tinychat](http://tinychat.com/wkbrdr16).
- f. A profile on the website spycam.forumup.dk in the name of wkbrdr16. The profile was created on December 19, 2011. No posts were made as of May 14, 2012.

- g. Two posts made by wkbrdr1994 on the website adultsearch.com. Wkbrdr1994 posted comments on May 3, 2012 regarding two different massage parlors in Great Falls, Montana. Wkbrdr1994 wrote that he first went to Touch of Klass Massage Studio, and then to Tokyo Massage. He indicated that he had a massage, and paid for sexual services afterwards.
34. C3/CEIU sent DHS Summons 366/12 to Optimum Online/Cablevision on May 21, 2012 for the IP address 174.44.165.69 on June 23, 2011 at 00:42 GMT, which was the most recent log data provided within the return from Stickam. C3/CEIU received a response from Optimum Online/Cablevision on May 24, 2012. Optimum Online/Cablevision indicated that the subscriber of the high speed internet service is:
- Account #: 8313200310361838
Subscriber: Aaron Thompson
Address: 418 1/2 Hayes Ave.
Helena, MT 59601-6149
Telephone #: 406-461-3090
Billing Address: 2769 Stacia Ave., Helena, MT. 59601-6411
35. The subject IP address was obtained on December 28, 2010 and released on October 10, 2011. The account appears to have been closed on October 14, 2011.
36. C3/CEIU determined that Aaron Luke THOMPSON was previously arrested by the FBI and convicted for distribution and possession of child pornography. THOMPSON's Sex Offender ID Number is MT02562420THOAAR. Information on THOMPSON'S federal case shows he was sentenced to 44 months incarceration and 36 months supervised release. THOMPSON'S parole was revoked on April 13, 2007 and received 6 months incarceration with 30 months supervised release.

37. After the initial evidence disk was sent to RAC Helena, C3/CEIU stated that they had another video that had been uploaded to the "falkovideo" site. C3/CEIU sent RAC Helena the video that they stated was uploaded on May 23, 2012. The video was listed as "0331" and depicted an adult and a prepubescent female in a green dressing room walking around with the females genitalia exposed.
38. On Aaron THOMPSON'S Notice for Offender Verification, where he provides update information for being a sex offender, on October 14, 2011 he shows his new and primary address as 2769 Stacia Ave., Helena, MT. 59601. The prior address crossed of is 418 1/2 Hayes, Helena, MT., 59601. The form shows THOMPSON currently working at Jewett Excavating Inc. HSI database searches also confirm his current address as 2769 Stacia Ave., Helena, MT. 59601, and his former address at 418 1/2 Hayes Ave., Helena, MT, 59601.
39. Information was sent from C3/CEIU to HSI RAC Helena, Montana, containing material for the above case. Included in the material, was a sanitized picture of the green family dressing/bath room. This picture was sent around to the Helena, Montana Police Department and FBI office, and employees from both agencies stated that it was from the Capital City Health Club in Helena, Montana, and it was from the family dressing rooms near the swimming pool.
40. On May 29, 2012, HSI Special Agent Reller and FBI Special Agent Damuth and ASAC Robert Lasky went into the Capital City Health Club in Helena, Montana and confirmed that the family dressing room near the swimming pool and day care was the one from the videos that had been uploaded to "Falkovideo". No recording device was found when law enforcement looked at the dressing room, or other dressing rooms in the area. Agents determined the recording device was hidden in the room and the individuals were secretly recorded.
41. A search for Aaron THOMPSON was conducted in Facebook, and his Facebook page was identified
"http://www.facebook.com/aaron.thompson.3726". THOMPSON is identified by his picture on the Facebook page. Agents compared the

image from the Facebook page and determined the man portrayed on that page matched the man portrayed by photograph in his background information, sexual offender registry, and from a picture provided by Capital City Health Club. Wakeboarding is listed as an activity on the page.

42. In Affiant's training and experience, Affiant has learned that Google Inc. provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Google Inc. allows subscribers to obtain e-mail accounts at the domain name "gmail" like the e-mail accounts listed in Attachment A. Subscribers obtain an account by registering with Google Inc. During the registration process, Google Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google Inc. are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google Inc. subscribers) and information concerning subscribers and their use of Google Inc. services, such as account access information, e-mail transaction information, and account application information.
43. In general, an e-mail that is sent to a Google Inc. subscriber is stored in the subscriber's "mail box" on Google Inc. servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google Inc. servers indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google Inc.'s servers for a certain period of time.
44. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google Inc.'s servers, and then transmitted to its end destination. Google Inc. often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google Inc. server, the e-mail can remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue to be available on Google Inc.'s servers for a certain period of time.
45. A sent or received e-mail typically includes the content of the

message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google Inc. but may not include all of these categories of data.

46. A Google Inc. subscriber can also store files, including e-mails, address books, contact or buddy lists, calendar data, pictures, and other files, on servers maintained and/or owned by Google Inc.
47. Subscribers to Google Inc. might not store on their home computers copies of the e-mails stored in their Google Inc. account. This is particularly true when they access their Google Inc. account through the web, or if they do not wish to maintain particular e-mails or files in their residence.
48. In general, e-mail providers like Google Inc. ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).
49. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google Inc.'s website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers

or other devices were used to access the e-mail account.

50. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.
51. In Affiant's training and experience, evidence of who was using an e-mail account may be found in address books, contact or buddy lists, e-mail in the account, and attachments to e-mails, including pictures and files.
52. A preservation letter for content was sent to Google Inc., for the account on wkbrdr1994@gmail.com, on June 11, 2012.

**INFORMATION TO BE SEARCHED AND THINGS TO BE
SEIZED**

53. Affiant anticipates executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

54. Based on the foregoing, Affiant requests the court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by

18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

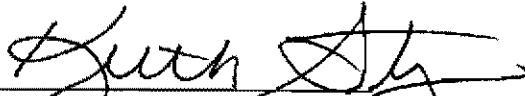
55. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



Aaron M. Reller, Special Agent
Homeland Security Investigations

Subscribed and sworn
before me this 27 of
August, 2012



The Honorable Keith Strong
United States Magistrate Judge